亚马逊云科技 | Deloitte.


# 制药行业客户在云上的计算机化系统验证最佳实践

**2021年10月**

# 目录

# 责任声明

客户有责任对本文档中的信息进行独立评估。本文档：(a) 仅供参考，(b) 代表当前的亚马逊云产品和德勤计算化系统验证CSV实践，如有更改，恕不另行通知;并且 (c) 不对亚马逊云科技和德勤，及其关联公司的供应商或第三方许可证机构做出任何承诺或保证。亚马逊云产品或服务“按当前运行模式”提供，没有任何明示或暗示的保证，陈述或任何形式的条件。本文档不是亚马逊云科技以及德勤与客户之间的任何协议的一部分，也不会对其进行修改。

# 1. 概述

## 引言

随着企业数字化转型脚步的加快和云技术的发展和进步，越来越多的企业将自身拥有的传统IT服务模式，转变为基于虚拟化技术建立的云模式。

目前，采用云计算已经成为企业IT实践的新常态。自2006年亚马逊云科技(Amazon Web Services)提出云计算服务以来，历经十几年的发展，云计算技术愈加完善，并且逐步增加了对行业的支持，为企业带来了诸多便利。在业务敏捷、成本优化、运营收益、敏捷运维、合规性等方面，体现了巨大优势。在生命科学行业，如何将云的优势转化为企业的竞争优势，成为了管理者和决策者值得思考的议题。

对于制药企业来说，本地储存庞大且持续增长的用户档案和信息会产生巨大的花费。而现在人口的急速扩张和平均寿命的增加扩大了制药企业储存数据的成本负担。迁移到云端意味着制药公司可以卸下相关负担，不需要再持续购买或维护自己的本地设备，例如过时的硬件和软件系统，以及不断需要更新的应用程序。企业的内部系统不仅在不断的更新和贬值，随着时间的推移，它所面对的安全问题更是与日俱增。在制药公司中，很少有公司内部的IT部门能够自己管理这些事物。而“临时管理员”对于信息安全更是一个潜在的威胁，他们无法提供定期的软件升级服务。将企业数据迁移到云端可以帮助公司专注于医疗行业，提高企业敏捷性而非IT技术。

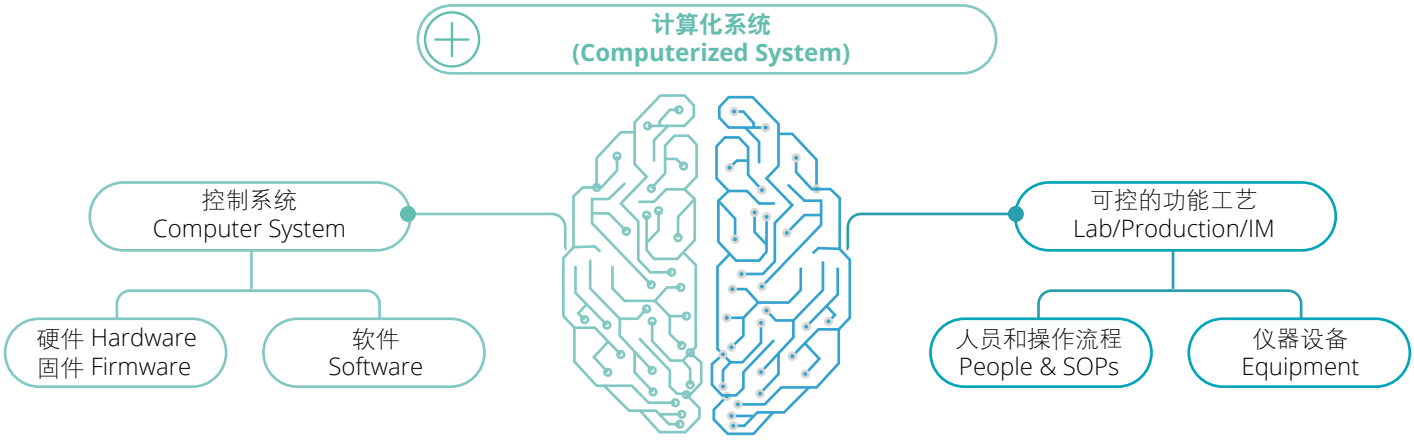
通过亚马逊云科技优质的云服务和功能并结合德勤对软件的更新进行集中管理，发布和技术支持，可以帮助企业降低数据储存的总体成本，消除计算机系统性能下降所带来的麻烦，同时提高企业的工作效率。另外德勤多年海内外制药行业计算机化系统验证(Computerized System Validation 计算机化系统验证)的项目经验，为制药企业提供从业务发展到技术框架方面的建议，帮助企业进行数字化转型。在一个法规和市场不断变化和创新的市场中，亚马逊云科技和德勤的技术支持是企业合规运营和长久发展的重要保证。

本文将详细介绍亚马逊云科技云服务、德勤计算机化系统验证技术支持，云上基础架构的搭建、验证和确认、以及质量管理体系的运行和维护流程。同时本文介绍了如何在云端构建新的SAP系统或迁移已有SAP系统到亚马逊云上基础架构，如何应对法律法规并确保云上基础架构、服务、业务的合规性以及数据的完整性。

## 制药行业GxP计算机化系统验证简介

计算机化系统验证，是采用科学的方法，对与药品质量安全密切相关的计算机化系统各个组成部分在全生命周期中进行持续、合理和有效的评估与文档记录，以确保和证明该系统是能符合各项GxP法规和预定用途的，产品能确保患者安全和质量要求，与产品质量有关的数据完整可信。计算机化系统的范围包括：硬件、软件、外围设备、操作人员、相关文件资料，如操作手册、SOP等。

**图1：计算机化系统的范围**




2019年新版《中华人民共和国药品管理法》的颁布对药品生产企业在从事药品研制、生产、经营、使用和监督管理等方面提出了更高的要求。我国已在2015年颁布了《药品生产质量管理规范 (2010年修订)》的《计算机化系统》和《确认与验证》两个附录，提出了药品生产企业信息化建设中需要依从的原则与目标。完备的计算机化系统建设不仅是企业信息化水平的体现，与质量管理息息相关，是企业合规运营、长久发展的重要保证。

## 生命科学行业云上部署计算机化系统挑战

生命科学行业一直是各个国家、地区重点关注、大力扶植的领域，对国计民生的重要性毋庸置疑。世界各地，也先后发布了涵盖研发、临床、制造、生产和销售等各个阶段的法律法规和指南。生命科学行业正加大数字化转型力度，云技术的应用极大地提高了企业服务的可扩展性，云供应商提供了更可靠的技术保障。但是云计算对制药行业GxP合规性挑战也成为生命科学行业选择云服务的疑虑。

对于全球化制药企业客户，GMP是大家公认的行业质量控制的规范，对于国内客户，计算机化系统验证计算机化系统验证是大家都要遵守的监管要求。本文立足亚马逊云科技的云计算，针对《药品生产质量管理规范 (2010年修订)》的附录《计算机化系统》和《确认与验证》的要求，结合德勤多年的海内外制药行业计算机化系统验证项目经验的积累，帮助企业在云上构建合规的生命科学应用，为药品生产企业提供从业务发展到技术框架方面的探讨和建议，为企业数字化转型提供催化剂。本文把需要遵守国内计算机化系统验证要求的制药企业应用系统，统称为计算机化系统。


DOCTOR
HS
HN
OH

# 2. 亚马逊云上基础架构的确认和运维

使用亚马逊云上基础架构作为GxP计算机化系统的环境时，医药企业用户根据安全责任共担矩阵，需要对自己负责的部分包括亚马逊云上基础架构进行确认和确认状态的保持。并在整个生命周期过程中有文档和记录。

结合亚马逊云科技和德勤各自在生命科学领域的实践积累，我们在本章针对合规要求提出了行业最佳实践与技术落地的方法。从评估与管理、项目实施和运行维护三个阶段分别阐述云上基础架构的合规性确认和运维流程。

## 评估和管理

### 供应商评估和管理

供应商的识别和管理是确保产品质量的重要前提条件之一，对于云服务供应商的选择尤甚。供应商评估和管理分为三个部分：识别供应商、供应商评估和建立供应商服务协议。

#### 识别供应商

为了保障安全、数据完整性和产品质量，企业在选择云供应商和其提供的服务/产品的时候应从以下几个方面进行评价：

- 技术能力，服务可靠性（备份和恢复、业务连续性）；
- 架构可扩展性，安全性（访问安全、数据安全、数据隐私、数据所有权、监控）；
- 合规要求。

**安全**

亚马逊云是一个安全持久的技术平台，已获得很多行业认可的认证和审核如：PCI DSS Level 1、ISO 27001、FISMA Moderate、FedRAMP、HIPAA、SOC 1（之前称为 SAS 70 和/或 SSAE 16）、SOC 2 的审核报告。

我们的服务和数据中心拥有多层操作和物理安全性，以确保客户数据的完整和安全。 请访问安全合规中心了解更多。

**备份与还原**

亚马逊云科技可以提供这方面的帮助。我们提供了丰富的存储服务、数据传输方法和联网选项，以构建具备无与伦比的持久性和安全性的数据保护解决方案。亚马逊云科技的基础架构多可用区设计的特点，也满足了客户同城灾备的需求，而中国的北京和宁夏两个具有同样架构的区域，可以满足客户异地容灾病实现自动化的灾备和恢复的需求。

### 供应商评估

为了保障安全、数据完整性和产品质量，所有参与使用和管理GxP计算机化系统的公司都应符合当地法律法规，并定期进行相应的供应商评估和审计。评估应考虑：供应商的质量管理体系、供应商的能力、安全性等。

对于审计在计算机化系统中使用亚马逊云科技产品的医药企业客户，评估系统安全性和数据完整性控制以及系统开发生命周期的持续有效性非常重要。为了对亚马逊云科技产品的使用情况进行有效的审计，医药企业的IT审计人员应熟悉在计算机化系统中亚马逊云科技产品的配置和使用。

对医药企业客户的审计，通过对该企业计算机化系统的某一时刻合规性的检查，确认其是否可以持续提供满足要求的服务。企业应该设立专业的质量保证人员，制定外部/内部审计计划，时刻警惕不良情况的发生。

亚马逊云科技运营行业领先的管理控制框架，该框架符合商业 IT组织当前的质量、安全性和信任标准。由合格的第三方审计人员定期进行亚马逊云科技控制的合规性评估，并将这些评估中的合规性报告提供给客户，以使他们能够评估亚马逊云科技作为供应商的服务能力。亚马逊云合规性报告指明了亚马逊云产品和评估区域的范围，以及评估者的合规证明。

**表1：亚马逊云合规报告**

| 控制机制 | 评估条件 | 审计人员 | 合规报告 |
|---|---|---|---|
| ISO 27001 | ISO/IEC 17021 及 27006 | CertifyPoint | https://aws.amazon.com/compliance/iso-27001-faqs/ |
| ISO 27017 | ISO/IEC 17021 及 27006 | CertifyPoint | https://aws.amazon.com/compliance/iso-27017-faqs/ |
| ISO 9001 | ISO/IEC 17021 | CertifyPoint | https://aws.amazon.com/compliance/iso-9001-faqs/ |
| SOC 1<br>SOC 2<br>SOC 3 | AT 801 &<br>AT 101 控制，TSP 100 部分，<br>信任及证明 | | https://aws.amazon.com/compliance/soc-faqs/ |
| FedRAMP/<br>NIST 800-53r4 | NIST 800-53a | Veris Group | https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/ |
| PCI-DSS v3.1<br>Level 1 | PCI DSS 安全审计流程 | Coalfire | https://aws.amazon.com/compliance/pci-dss-level-1-faqs/ |

其他在线资源可用于为客户提供有关亚马逊云科技安全流程以及亚马逊云科技产品当前和过去性能历史的透明性：

- 亚马逊云风险和合规性白皮书：

  https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

- 亚马逊云安全流程白皮书概览：
  https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
- 亚马逊云服务运行状况控制面板和状态历史：
  http://status.aws.amazon.com/

GxP客户应考虑更新其供应商评估流程，以确保所有供应商类别均可适应亚马逊云科技的产品。对于以前在非GxP系统中使用过亚马逊云科技产品的 GxP 客户，他们对亚马逊云科技的GxP供应商评估还应包括对那些非GxP系统的性能历史审查，包括归因于亚马逊云科技且客户无法通过其解决方案架构解决的任何与系统相关的问题。

企业可以通过亚马逊云科技的服务Amazon CloudTrail的建议实施落地。使用Amazon CloudTrail对企业的亚马逊云 账户进行监管、合规性检查、操作审核和风险审核的服务。借助 CloudTrail，客户可以记录日志、持续监控并保留与整个亚马逊云基础设施中的操作相关的账户活动。CloudTrail提供亚马逊云账户活动的事件历史记录，这些活动包括通过亚马逊云科技管理控制台、亚马逊云开发工具包、命令行工具和其他亚马逊云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

德勤咨询可提供审计咨询服务，以确认亚马逊云科技作为云供应商符合ISO、SOC等的要求。

**供应商服务协议**

供应商提供产品或服务时，医药企业客户应当与供应商签订正式协议，明确双方责任。供应商协议应包括：

- 服务水平协议（SLA）：描述了获得服务信用的条件和提交索赔的过程。
- 在线服务条款：包括IT服务交付物、双方的角色和职责、质量管理的要求包括隐私、数据安全和保护、文档和数据保留、安全控制和监控、物理资产和数据资产的所有权和管理、事故和故障管理、供应商绩效管理和提升、职业道德和财务要求、业务连续性、可接受的使用政策、遵守法律及服务停止等条款。

为了确保基础架构组件符合最终用户的要求，云供应商必须保证实施受控流程，以确保满足服务级别协议 (SLA) 。有GxP要求的组织需要根据满足指定要求的能力来评估和选择其潜在的供应商、承包商和顾问。一旦客户执行了产品评估并确定亚马逊云科技产品可以满足其GxP系统架构的要求，就可以执行供应商评估，以确保亚马逊云科技可以根据其发布的接口规范和SLA可靠地交付亚马逊云产品。

亚马逊云科技作为云供应商，在中国提供北京区域和宁夏区域，这两个区域所获取的资质参见表 4 亚马逊云在中国的合规遵从的描述。两个区域提供的服务水平协议 https://www.amazonaws.cn/legal/sla/

**表2：亚马逊云服务水平协议列表**

| 区域 | 服务名称 | SLA |
|---|---|---|
| 北京区域 | Amazon Compute | 99.99% |
| | Amazon S3 | 99.9% |
| | Amazon RDS | 99.95% |
| 宁夏区域 | Amazon Compute | 99.99% |
| | Amazon S3 | 99.9% |
| | Amazon RDS | 99.95% |

### 云产品服务评估

医药企业应根据既定用途对亚马逊云科技产品和服务进行选型。首先亚马逊云科技提供完整的产品和功能，同时亚马逊云科技提供通过优良架构帮助客户在亚马逊云上构建应用系统，亚马逊云科技还提供了丰富的亚马逊云科技 APN 合作伙伴网络以及Marketplace，为客户提供满足各类需求的云端生态的产品和解决方案。

- 亚马逊云科技在中国提供的产品：https://www.amazonaws.cn/products/
- 针对产品的使用文档参见文档中心：https://aws.amazon.com/documentation/

亚马逊云科技的良好框架帮助客户理解的方式建议如何在亚马逊云上构建系统。通过使用框架，客户能够学习在云中如何按照最佳实践在设计应用以及如何操作可靠、安全、高效和具有成本效益的云中系统。该框架提供了一种方法来一致地根据最佳实践度量客户的架构并确定需要改进的领域。审查体系结构的过程是关于体系结构决策的建设性对话，而不是审计机制。我们相信拥有架构良好的系统将大大增加业务成功的可能性。

**表3：亚马逊云优良架构框架的五个支柱**

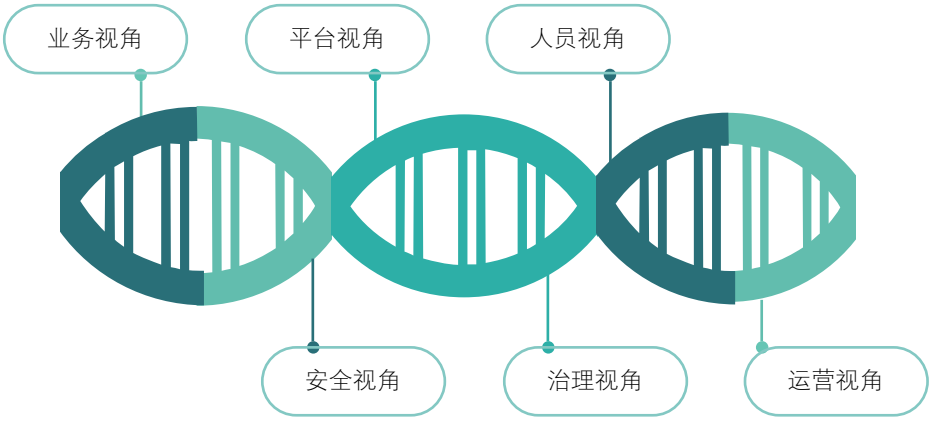
| 名称 | 描述 |
| --- | --- |
| 卓越运维 | 能够运行和监控系统以交付业务价值，并持续改进以支持流程和过程。 |
| 安全 | 在通过风险评估和缓解策略交付业务价值的同时保护信息、系统和资产的能力。 |
| 可靠性 | 系统从基础设施或服务中断中恢复、动态获取计算资源以满足需求以及减轻诸如错误配置或瞬态网络问题等中断的能力。 |
| 性能效率 | 能够有效地利用计算资源以满足系统需求,并能够随着需求的变化和技术的发展维护系统运行的效率。 |
| 成本优化 | 能够以最低的价格运行系统以交付业务价值。 |

亚马逊云科技 APN 合作伙伴网络 (AWS Partner Network，简称 APN)是亚马逊云科技推出的一项全球合作伙伴计划，它针对采用亚马逊云科技开展业务的技术类企业与咨询类企业。超过90%的财富100强企业在使用APN合作伙伴提供的解决方案与服务。APN将通过为客户提供持续更新的业务、技术与市场方面的重要支持，全力帮助客户建立与推广云业务，并最终取得成功。

AWS Marketplace China 提供了数以百计的业界领先的合作伙伴的产品，包括反恶意软件、web应用程序防火墙和入侵保护。这些产品补充了亚马逊云科技提供的工具和功能，使客户能够部署全面的安全体系结构，并在云环境和本地环境中实现更无缝的体验。

### 风险管理

风险管理应当贯穿计算机化系统的生命周期全过程，应当考虑安全、数据完整性和产品质量。亚马逊云科技采用框架(AWS CAF)提供了支持组织中每个单元的指导，以便每个领域都了解如何更新技能、调整现有流程和引入新流程，以最大限度地利用云计算提供的服务。全球成千上万的组织已经成功地将他们的业务迁移到云上，并依靠AWS CAF来指导他们的工作。CAF从如下的六个维度帮助客户梳理现状，建立云端规划。通过此框架，客户可以平衡风险与机遇，识别在亚马逊云上部署应用的风险，采取措施缓解风险，指定流程和应对机制并记录风险评估的工作。




亚马逊云还可以从设计阶段，就开始对可能导致风险的因素进行处理。针对在亚马逊云中运行的基础设施、操作系统、服务和应用程序，设计安全实践概述了控制责任、安全基准的自动化、安全配置和客户对控制的审计。此设计具有标准化、自动化、规范且可重复的特点，可根据常见的使用案例、安全标准和审计要求跨多个行业和工作负载进行部署。

设计安全实践方法可以实现以下目标：创建强制性功能，使不可修改这些功能的用户无法对其进行覆盖。建立可靠的控制操作；启用持续的实时审核；监管策略的技术脚本编写。
设计安全实践的结果是获得一个支持环境的安全、保证、管理和合规性功能的自动化环境。借此，客户可以可靠地实施之前仅在策略、标准和规章中写入的内容。此外，客户还可创建强制性的安全和合规规则，而这些规则反过来帮助创建一个适用于客户的亚马逊云环境的可靠的功能性管理模式。

相关的亚马逊云服务包括：Amazon KMS 加密可实现强制对 Amazon S3 对象存储进行服务器端加密，IAM服务实现资源权限管理，账号访问操作的日志记录在CloudTrail， Amazon CloudFormation 可以把安全设计的内容形成模板并做到自动化部署。

亚马逊云还有Trusted Advisor服务[6]，这是一个在线工具，可为客户提供实时指导以帮助客户按照亚马逊云科技最佳实践预置资源。无论是创建新工作流、开发应用程序还是在持续改进期间，都可以利用 Trusted Advisor 定期提供的关于成本优化、安全、性能、容错和服务限制五个方面建议，来确保以最佳方式预置解决方案。亚马逊云的“良好架构”[7]帮助云架构师为其应用程序构建安全、高性能、具有弹性和高效的基础设施。基于安全性、可靠性、性能效率、成本优化和卓越操作这五个基础支柱，此框架为客户和合作伙伴提供了一种评估架构的一致方法，并实施能够在使用中扩展的设计。

### 人员

参与开发、验证、维护、使用和管理GxP计算机化系统的人员应根据角色和职责进行充分的教育和培训并记录，以获得从事工作应具备的相应的资质和能力。

如果工作职能包括在计算机化系统中使用亚马逊云科技产品，那么在雇用和/或培训人员时应考虑亚马逊云科技产品的经验水平。系统访问级别和执行的工作职能与确定所需的经验水平相关。

亚马逊云科技作为提供云服务的供应商，没有责任确保医药企业客户的员工具有相当的教育水平、经验和资质。但是亚马逊云科技和亚马逊云科技APN合作伙伴网络提供了关于亚马逊云科技产品的一系列初始和进行中培训和认证，包括：

- 在线文档https://aws.amazon.com/documentation/
- 教学视频 https://aws.amazon.com/training/intro_series/
- 自主进度动手实验室 https://aws.amazon.com/training/self-paced-labs/
- 活动和网络研讨会 https://aws.amazon.com/about-aws/events/
- 课程和研讨会： https://aws.amazon.com/training/course-descriptions/
- 合作伙伴培训： https://aws.amazon.com/partners/training/
- 专业证书：https://aws.amazon.com/certification/

## 项目实施

ISPE GAMP5将基础架构软件划分为第一类软件系统，使用亚马逊云科技产品/服务构建的云上基础架构的确认应遵循GAMP5指南中的计算机化系统完整生命周期过程，由医药企业对其整个生命周期的所有活动负责。对于云上基础架构搭建项目的实施和验证，可由医药企业自己的实施和验证团队进行，或者由其他有资质的实施和验证供应商完成。

德勤具有丰富的系统实施和验证经验，可为药企云上基础架构和业务应用提供合规咨询服务。包括云上基础架构实施和验证咨询服务，云上GxP业务应用实施和验证咨询服务，云管理体系搭建咨询服务。

对于云上基础架构的实施和验证，主要包括四个阶段：计划阶段、设计开发阶段、部署验证阶段和报告交付阶段。

尽管亚马逊云科技产品通常与SDLC方法（如DevOps）相关联，但SDLC（如瀑布和 V 模型）受到完全支持。本节基于德勤的项目实施 SDLC 示例，向在GxP系统中使用亚马逊云产品的客户解释一些注意事项。

### 计划

在项目初始规划阶段，医药企业需定义项目范围、验证与确认的原则、策略方案、验证活动、项目交付物和生成项目交付成果的人员和责任，包括SOP、规范和验证文档等。

### 设计开发

云上基础架构的规范文档，包括需求规范和技术设计规范。需求规范应结合医药企业系统所有者/业务用户的使用需求、GxP应用程序所要求的支持功能和监管部门对于云部署的监管和法规，由医药企业用户制定。用户需求最初是在设计阶段创建的，应有对系统应该做什么和对功能性及非功能性需求的描述。用户需求规范是项目中所有确认工作的基础。在用户需求规范里的具体需求都被赋予了一个唯一标识。通过对业务流程进行全面的分析，得到用户需求说并映射到功能说明。配置说明和设计说明作为技术的说明文件，阐述了系统实施的技术细节。对于开发的代码中较高风险的，代码审查必须文档化，以确保其符合行业内标准。软件的定制化和编码过程依据GAMP5中的相关指导。

医药企业负责云基础架构设计的架构师在规划、规范和设计阶段，除基础功能需求外，还应考虑：

- 数据在保存和传输过程中的加密性；
- 系统的高可用性；
- 备份和恢复策略，定义恢复时间目标RTO和恢复点目标RPO；
- 审计追踪；
- 安全－权限管理、网络安全、数据保护；
- 监控。

亚马逊云“优良架构”(参见4.1.2云产品服务产品评估) 可以在生命科学应用的架构设计，运营方面提供建议。

亚马逊云可以提供多种服务来帮助生命科学企业实现DevOps，而且这些服务的设计初衷是与亚马逊云配合使用。这些工具可以自动执行任务，帮助团队大规模管理复杂环境，并使工程师能够控制的DevOps实现的高速度发布。从而在云上实现企业在应用开发，验证、确认以及自动化部署方面的不断改进。

Amazon OpsWorks、Amazon CodeCommit 和 Amazon CodePipeline 等亚马逊云科技产品为系统工程师提供了灵活的可配置工具，可帮助他们满足其独特的组织要求，同时还简化了软件开发活动的SDLC控制的实施。在客户完成开发并准备好将其 GxP 系统部署到验证、生产或其他环境中之后，亚马逊云科技产品 (例如 Amazon Machine Images(AMI)、Amazon CloudFormation、Amazon CodeDeploy 和 Amazon Elastic Beanstalk) 将使一致且受控的部署变得容易且可重复。这些工具还能够创建从网络堆栈到数据库、从存储卷到计算实例的整个系统环境的版本控制。可以保留这些版本控制的副本，以用于归档和更改管理，或用于预置新的开发/测试环境以便执行持续的开发或问题排查。这种持续开发和持续部署的新模型是众多行业中如此多客户使用亚马逊云产品创新业务的主要原因之一。

为了帮助客户优化变更流程，亚马逊云科技提供了新服务和新功能特性发布的信息。针对已有服务的变更，亚马逊云科技通过健康仪表盘发布给客户，同时发送邮件通知到客户的注册邮箱。

亚马逊云端的自动化部署主要通过Amazon CloudFormation服务实现，该服务可对亚马逊云资源进行建模和设置，以便节省时间。CloudFormation通过模板调度资源和服务，设置和配置这些资源并处理所有依赖关系。

亚马逊云提供多种开发工具，主要包括API，SDK，和命令行工具CLI。亚马逊云的服务提供完整的API及文档，协助开企业基于亚马逊云服务开发各种应用。SDK支持C++, Go, Java, JavaScript, .Net, PHP, Ruby等开发语言。亚马逊云提供各种IDE的toolkit，帮助开发提高开发效率。包括Toolkit for Eclipse, JetBrains, Visual Studio, Visual Studio Code, PowerShell和Visual Studio Team Services。AWS Command Line Interface(AWS CLI) 是一种开源工具，仅需最少的配置就可以从常用终端程序中的命令提示符开始使用基于浏览器的亚马逊云科技管理控制台提供的相同功能。

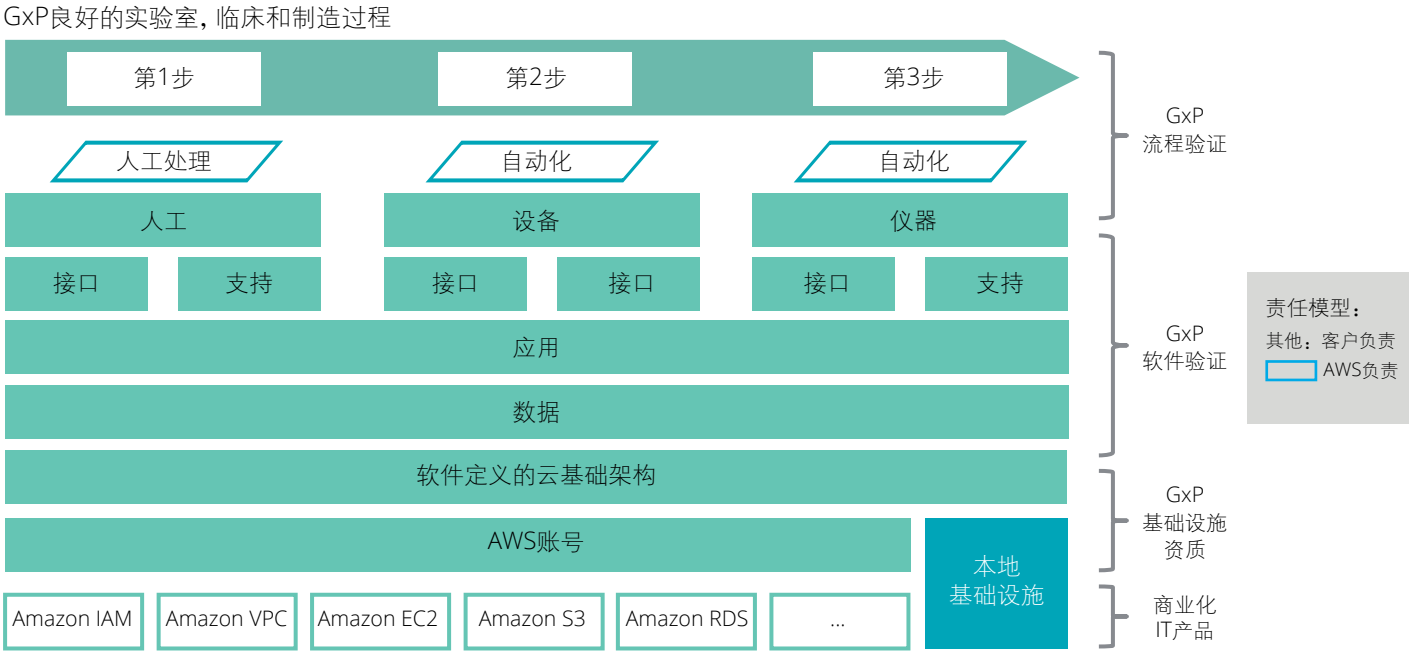
### 部署和验证

根据基础架构的规范文档，完成亚马逊云上基础架构的部署和配置。云上基础架构是采用标准的或者商用的组件搭建而成的，和应用的业务流程没有直接关系，需要对部署好的云上基础架构进行安装确认 (IQ) ，运行确认 (OQ) 和性能确认 (PQ) 。

- 医药企业用户进行安装确认（IQ），以确保云上基础架构的关键配置、设置与记录的规范相匹配。
- 根据风险评估的输出和预定义的验收标准，执行功能测试或运行确认（OQ），以验证关键云上基础架构组件是否按预期运行。
- 对用户需求和SOP进行性能确认（PQ），以验证系统部署和配置符合用户及企业的要求。

针对计算机化系统验证的需求，亚马逊云科技为企业提供了清晰的责任模型。

**图2：计算机化系统验证中的责任模型**




针对部署在亚马逊云的合规应用，建议用户采用以下实践方式：针对云服务，优化质量管理体系，优化架构设计指引，制定云上开发流程，制定云上验证流程，制定云上确认流程，制定自动化部署流程，针对云服务，优化变更流程。

### 报告和交付

完成验证活动后，汇总测试结果，并在总结报告中确认总体验收标准。云上基础架构所有者和管理员应在确认活动完成后，遵循医药企业自身质量管理体系对其进行管理，以维护其确认合格的状态。

成功完成基础架构确认活动通常是开始GxP应用程序验证活动的入口准则。

### 运行维护阶段

亚马逊云上基础架构投入使用后在使用过程中要继续维持其确认合格的状态。在运行维护过程中，医药企业客户需要建立一系列支持流程。包括：用户与权限管理、变更和配置管理、问题与事件管理、业务持续性管理等。

德勤咨询可根据医药企业自身质量管理流程体系特点，提供云上基础架构运行和维护支持流程补充或建立的咨询服务。

Web 服务技术与现代的自动部署实践相结合，可以通过允许单个系统组件的更新（系统停机时间极短，通常不需要停机）或打破依赖关系来进行更新，从而提高进行连续开发的系统的速度和弹性。只要 API 接口规范没有更改，客户就可以与系统交互并相信 (但需要验证) 正在使用的功能可用。使用亚马逊云科技产品的客户可以受益于Web服务API的各个方面，尽管客户仍必须构建其系统以应对API中断。基于API的系统还可以与IT服务管理系统或变更控制系统集成在一起，从而提供具有 GxP 质量署名的软件开发和部署管道的完全集成。

亚马逊云科技提供的云服务丰富广泛，其中包括很多用来实现系统运维的服务，包括监控，配置管理，主机管理，安全，备份容灾等；同时亚马逊云按需使用，按量付费的模式，改变了客户原本的IT投入方式，降低资金压力，针对医药企业，亚马逊云可以为业务实现敏捷提供支持。因此，选择全球大多数制药企业使用的亚马逊云计算平台，可以加速医药生产企业云化转型的历程，降低合规与安全风险。

使用Amazon CloudWatch 进行监控。CloudWatch提供相关数据和切实见解，以监控应用程序、响应系统范围的性能变化、优化资源利用率，并在统一视图中查看运营状况。CloudWatch 以日志、指标和事件的形式收集监控和运营数据，能够统一查看在亚马逊云和本地服务器上运行的资源、应用程序和服务。使用 CloudWatch检测环境中的异常行为、设置警报、并排显示日志和指标、执行自动化操作、排查问题，以及发现可确保应用程序正常运行的见解。

Amazon Simple Storage Service (Amazon S3) 是一种对象存储，它具有简单的Web服务界面，可用于存储和检索Web上任何位置、任意数量的数据。它能够提供 99.999999999% 的持久性，并且可以在亚马逊云科技中国各个区域间大规模传递大量对象。将存储资源向上和向下扩展以满足不断变化的需求，无需前期投资或资源采购周期。Amazon S3 可达到 99.999999999% (11 个 9) 的数据持久性，因为它会自动创建和存储跨多个系统的所有 Amazon S3 对象的副本。这意味着客户的数据在需要时可用，并可抵御故障、错误和威胁。Amazon S3 智能分层根据访问模式的变化为对象分层并自动实现成本节省。Amazon S3 是唯一可使客户通过 Amazon S3 数据块公有访问在存储桶或账户级别阻止对客户的所有对象进行公有访问的对象存储服务。Amazon S3 维护合规性计划 (如 PCI-DSS、HIPAA/HITECH、FedRAMP、欧盟数据保护指令和 FISMA) 以帮助客户满足法规要求。亚马逊云还支持很多审核功能以监控对 Amazon S3 资源的访问请求。

Amazon S3 Glacier 和 S3 Glacier Deep Archive 是安全、持久且成本极低的 Amazon S3 云存储类，适用于数据存档和长期备份。它们能够提供 99.999999999% 的持久性以及全面的安全与合规功能，可以帮助满足最严格的监管要求。

医疗保健等许多企业必须长期保留法规和合规性存档。Amazon S3 对象锁定可帮助客户设置合规性控制以满足目标，如 SEC 规则 17a-4(f)。

使用亚马逊云实现数据保护、备份归档和灾难，拥有传统IT无法比拟的巨大优势。云灾备具备以下优势：按需使用并付费，低成本；无独立购买使用维护各种软硬件；亚马逊云科技天然具有高可用高容错的架并提供相应服务供客户设计并实施容灾的架构；基于亚马逊云可以简便快速灵活地构建灾备站点。亚马逊云科技中国区提供两个区域，五个可用区，可以很方便的为客户提供两地三中心的企业级容灾架构。

亚马逊云备份和容灾设计服务包括存储服务Amazon S3，自动化模版服务CloudFormation，服务器迁移SMS，数据库迁移DMS，专线网络连接DX，数据离线迁移工具Snowball等。 Amazon S3服务可以用来备份基础架构的各类镜像、配置信息、数据库镜像、应用数据，并根据应用需要设置不同的访问权限，根据数据使用频率设计不同保存级别，根据生命周期设置归档等。亚马逊云科技中国区域有众多合作伙伴提供备份和容灾方案的工具。

有别于传统数据中心的运维模式，药品生产企业应该及时获得云计算厂商提供的事件报告和纠正及预防行动计划等信息，甄别波及范围并完成合适的风险评估，采取相应措施，更新/优化标准流程，保证合规应用的验证状态。

### 用户与权限管理

医药企业应对亚马逊云上基础架构的用户与权限进行管理。基础架构不同于应用系统，医药企业普通用户不会在日常工作中直接访问云上基础架构，而是通过应用系统读取或使用存储在基础架构上的数据。有权限对基础架构进行直接访问和操作的，通常是医药企业基础架构运维人员和基础架构管理员。

药企用户应对云上基础架构的用户和权限进行管理并建立相关的管理流程：

- 完整的权限审批流程，可以保证从源头就建立合适的安全机制，在云基础架构层面，有效控制数据访问的权限。
- 访问管理，依从最小权限原则，最大程度的避免非授权操作，降低风险。
- 密码管理，需要定期更换密码，规定密码复杂度，并妥善保存密码。
- 权限回收机制，制定合适的流程，在特定时间范围内处理访问权限。
- 安全监控与报警，任何非授权访问都应该被及时监控并报警，以便采取应对措施。

亚马逊云的IAM服务提供访问控制功能定义、执行和管理用户访问在亚马逊云服务政策。这些包括:身份和访问管理功能来定义个人用户账户权限，密码管理，角色定义与STS临时授权，多因素身份验证,包括基于硬件的身份验证器，集成、企业目录和联盟，以减少管理开销和提高用户体验，亚马逊云提供跨许多服务的本地身份和访问管理集成，以及与客户自己的任何应用程序或服务的API集成。CloudTrail服务可以对账号的使用情况进行记录与跟踪，结合CloudWatch和更多的服务，可以实现自动化的安全监控与管理。

### 变更和配置管理

云上基础架构的变更也应当根据预定的操作规程进行，操作规程应当包括评估、验证、审核、批准和实施变更等规定。按照规定的程序，以受控的方式实施计算机系统包括系统配置的任何变更。药企用户负责对云上基础架构进行变更的管理，负责验证和确认对基础架构功能和配置实施的更改。

Amazon Config 服务可供客户评估、审计和评价亚马逊云 资源配置。Amazon Config 持续监控和记录亚马逊云资源配置，并支持客户自动依据配置需求评估记录的配置。借助 Amazon Config，客户可以查看配置更改以及亚马逊云资源之间的关系、深入探究详细的资源配置历史记录并判断配置在整体上是否符合内部指南中所指定的配置要求。客户由此能够简化合规性审计、安全性分析、变更管理和操作故障排除。

亚马逊云为系统和运营管理提供一组服务，允许客户通过适当的管理和合规性来控制基础设施资源。客户可以使用 Amazon Systems Manager 快速查看和监控客户的所有资源并自动执行常见运营任务，如修补或状态管理。Systems Manager 提供统一的用户界面，客户可以在一个位置轻松管理客户的云运营活动。客户还可以使用Amazon CloudTrail记录组织内的用户活动，使用Amazon Config清查资源中的所有配置。

Amazon OpsWorks是一项完全托管的配置管理服务，用于托管和扩展 Chef Automate 和 Puppet Enterprise 服务器。借助 OpsWorks，客户无需安装和运营自己的配置管理系统，也不用操心其基础设施的扩展。它还可以与客户现有的 Chef 和 Puppet 工具无缝协作。OpsWorks 将自动修补、更新和备份客户的 Chef 和 Puppet 服务器，并维护其可用性。如果客户是 Chef 或 Puppet 现有用户，OpsWorks 是很好的选择。

### 问题与事件管理

医药企业用户应该对云上基础架构进行维护和监控，当出现问题或故障时，及时进行响应和纠正。医药企业用户应建立相应的管理流程，包括对问题或故障的识别、记录、评估、调查、解决和确认。

### 业务持续性管理

医药企业客户应该针对云上基础架构特点，进行业务持续性管理并建立相应流程，包括灾难恢复以及备份策略。

亚马逊云提供了丰富的存储服务、数据传输方法和联网选项，以构建具备无与伦比的持久性和安全性的数据保护解决方案。数据库备份方面，许多 亚马逊云 数据库服务 (关系和非关系) 都具有内置的自动备份功能，可以保护客户的数据和应用程序。数据生命周期管理方面：Amazon S3 提供不同的存储类，以可变成本存储不太频繁访问的数据。使用生命周期策略自动执行分层或按需执行此操作。使用 Amazon Storage Gateway 创建虚拟磁带库，并且不需要负责监管采购周期和容易出错的流程。借助云连接器和网关，客户可以开始将其本地数据备份到亚马逊云，以实现持久的数据保护。具有数据保留要求的组织可以使用 Amazon S3、S3 Glacier 和 S3 Glacier Deep Archive 进行低成本长期存储，该存储具有强制实施 WORM 控制的内置功能。

Amazon Backup 是一种完全托管的备份服务，可以使用 Amazon Backup 轻松集中和自动管理云中以及本地亚马逊云服务中数据的备份。使用 Amazon Backup，客户可以集中配置备份策略并监控 Amazon EBS 卷、Amazon RDS 数据库、Amazon DynamoDB 表、Amazon EFS 文件系统和 Amazon Storage Gateway 卷等亚马逊云资源的备份活动。Amazon  Backup可自动执行并整合之前按服务执行的备份任务，而无需创建自定义脚本和手动流程。Amazon Backup 提供完全托管的基于策略的备份解决方案，简化了备份管理，使客户能够满足业务和法规备份合规性要求。详细了解 Amazon Backup的优势、亚马逊云 存储和备份、亚马逊云科技 APN 合作伙伴网络、使用案例和客户案例研究以及如何从备份发展到存档和灾难恢复。


基础数据
78.93
65.91
89
89
65 --- 120
65 --- 120
56

# 3. SAP ERP在亚马逊云上的计算机化系统的验证和运维

本章以SAP ERP系统为例，概括介绍计算机化系统在云架构上的验证策略。在计算机化系统中使用亚马逊云产品的客户应对其亚马逊云账户中的所有软件验证活动或资格认证完全负责。由于亚马逊云科技不代表客户开发或管理应用程序，因此亚马逊云科技无法代表客户执行GxP验证或资格认证活动。

德勤咨询是SAP铂金级优秀合作伙伴，具有大量医药企业和多个云上SAP系统实施和验证经验。德勤咨询可以为医药企业新系统上云、系统迁移上云提供实施和验证咨询服务。

## 云上部署计算机化系统验证的背景及环境

成功完成亚马逊云基础架构验证活动是开始GxP应用程序验证活动的阶段门户，高效且严谨的计算机化系统验证方法论是确保制药行业计算机化系统合规的重要条件。

德勤根据多年的计算机化系统验证项目经验，结合信息化系统实施的EVD方法论，形成了通用的制药行业最佳业务实践。在验证团队和实施团队的工作最优化融合下，实现了计算机化系统验证过程与SAP系统实施的完美匹配与结合。本节首先将对SAP系统的本地配置和云上配置进行对比分析，再通过展示云上部署应用的计算机化系统验证实践案例，来具体说明德勤计算机化系统验证的框架。

### 制药行业执行计算机化系统验证的必要性

根据中国GMP2010修订版，在制药行业使用计算机化系统代替人工操作时，应当确保不对产品的质量、过程控制和其他质量保证水平造成负面影响，不增加总体风险。计算机化系统可以通过代替人工操作，提高工作效率，但是需要考虑这种替代或变革随之带来的风险，需全面考虑来自产品质量、过程控制及整个质量保证体系的风险。即无论大到变革、小到变更，在制药行业实施SAP系统的全流程中都要做好风险识别和风险评估工作，这是一切“变”的前提和刚性要求。

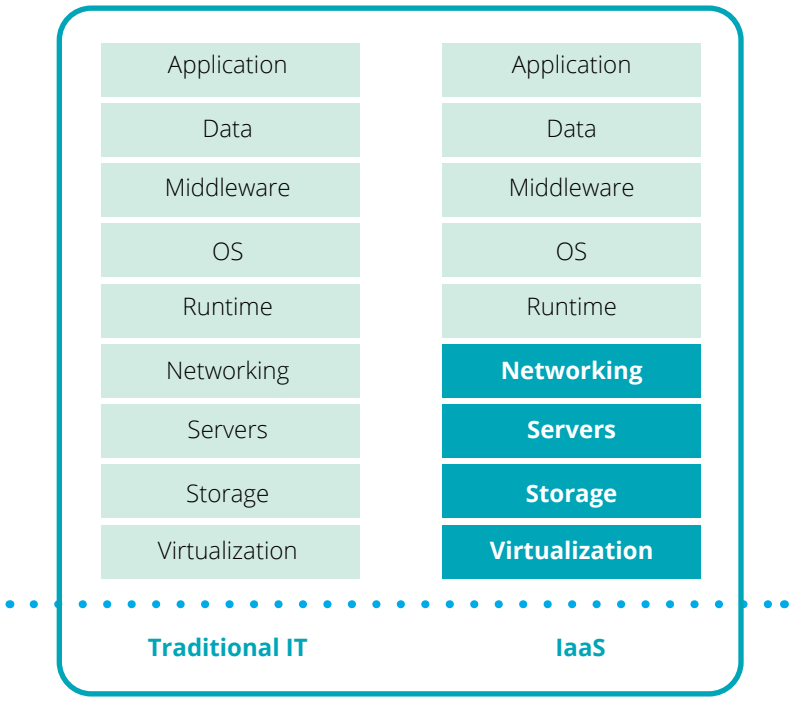
### SAP系统的不同部署版本

除了SAP S/4 HANA的部署 (On-Premise) 版本，SAP还提供了不同版本的部署方式：本地部署或云上部署。

- 本地部署
  拥有服务器等硬件以及软件所有权，且灵活性较高，可以根据企业具体需求进行个性化定制。然而，本地部署对前期投资的要求较高，包括购买或租用硬件、服务器和其他IT基础设施，还需考虑企业内部人员配备成本以及后续的运维成本。
- 云上部署
  云上部署前期投入成本低，与IaaS供应商签订合同从而将后续维护责任转移给供应商；精良的IT支持团队可以通过最新的前沿技术为客户提供更好的性能，云上部署具有高灵活性、高效率以及快速部署的优势。

### 传统IT模式与亚马逊云服务模式的区别

将现有SAP系统从传统IT基础架构迁移到亚马逊云端，部分IT基础设施确认工作将会转移给云服务商。下图展示了SAP系统迁移至亚马逊云端的过程，左侧为本地化部署需要做的合规性相关工作，右侧为系统迁移至云端后，云服务商负责的模块工作：




当虚拟化管理、数据存储和备份、网络架构、服务器和服务机房等工作转移给云服务商后，需要请云服务商提供以下信息：

- 确认文件：云服务商需要执行以上确认，并向使用方提供相关报告
- 管理体系：云服务商需要具备完整的管理体系，使用方需对云服务商进行审计用以确保其具有系统的确认、异常、变更、运维等管理能力。
- SLA: 将使用方转移给云服务商所提供的服务和管理进行说明，并需要把这些服务所能引起的风险点也列入协议中以明确责任。

综上可见，IaaS的部署是企业和IaaS服务商共同紧密合作完成的，因此IaaS服务协议就变得非常重要，一般情况下，除了常规法规条款外，协议应该重点考虑几方面因素：

- 符合GxP的法规需求，例如需要提供一系列SOP包括Change Management/ Incident Management等，并可以周期性地提供证据证明这些SOP被有效地执行
- 合规相关需求所涉及的内容应该被准确描述在SOW中，特别是交付物部分
- SLA服务除了常规服务条款也应该包含法规相关的内容，例如基于风险评估的变更管理（客户需要被及时通知），或是对内部审计和外部法规检查活动的配合。

## 在亚马逊云上基础架构搭建新的SAP系统

在云端与在传统IT基础架构上部署和验证计算机化系统的策略和方法是基本一致的。均应符合法律法规对计算机化系统验证的要求，根据GAMP5指南计算机化系统完整生命周期方式，系统软件类别分类、系统评估结论和风险评估进行系统验证。

GAMP5是国际制药工程学会 (ISPE) 和和一套在自动化环境下进行生产的指导原则的结合体，它遵循美国和欧洲监管要求。GAMP5是制药企业在计算机化系统验证领域应用广泛的并得到国际认可的指南。基于GAMP5，德勤团队提出了计算机化系统验证框架——V模型。

SAP实施过程将会被全面记录并测试，其中可能会影响药品的质量，安全，有效性，完整性功能和系统组件将会被验证，用来确保系统功能可以持续稳定运行，并满足法规要求以及企业业务操作流程。

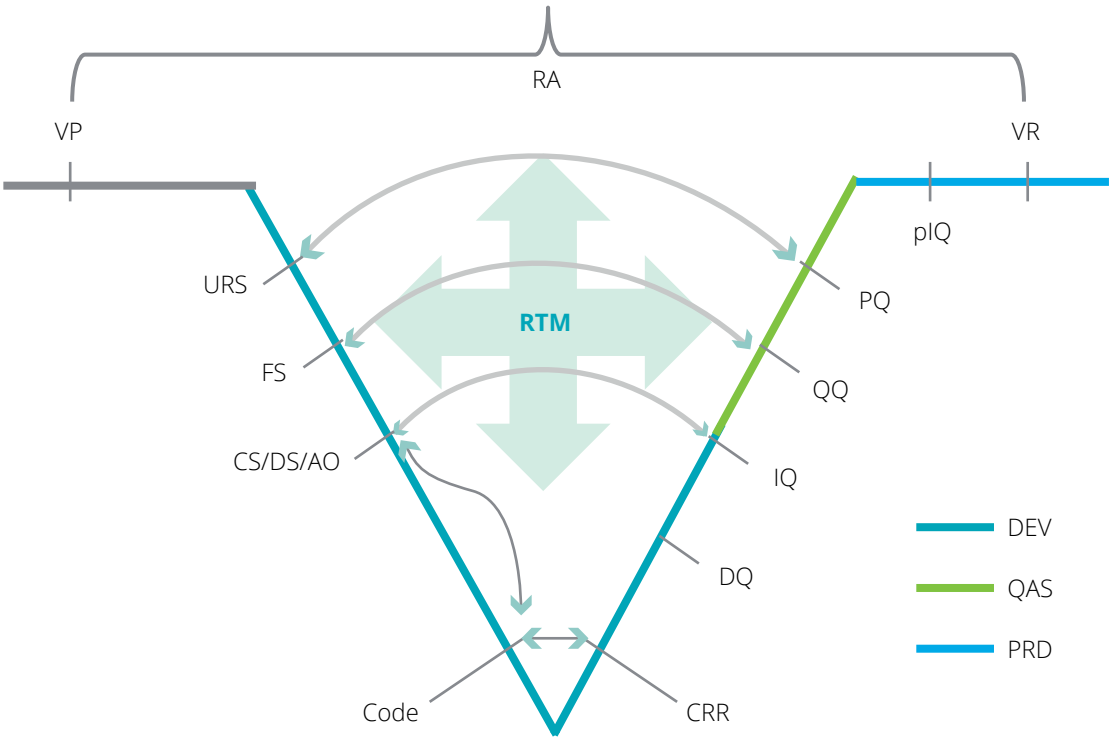
计算机系统验证根据以下构建:

- 系统影响评估
- 软件类别
- SAP系统的软件类别分类选择的验证生命周期策略
- 企业SOP，计算机化系统生命周期
- 风险评估的结果（作为验证方法的组成部分，验证团队将采取基于风险的方法，对SAP系统功能的风险水平进行评估。风险评估（RA）将对SAP系统验证范围内的流程或功能相关的法规和业务风险进行合理的评估并进行书面记录并交予管理层进行审批）。
- 风险评估(RA)中包括：
  - 供应商评估
  - 电子记录和电子签名评估
  - 基于用户需求 (URS) 的风险评估
- SAP 系统分为如下三个环境：
  - 开发环境(DEV)
  - 验证环境(QAS)
  - 生产环境(PRD)

开发环境(DEV), 验证环境(QAS)和生产环境(PRD)三个环境的安装是一致的。开发活动结束后，系统所有的最终设置和开发都将从开发环境(DEV)转移到验证环境(QAS)。在验证过程中发现的任何改变将在开发环境(DEV)和验证环境(QAS)环境做变更验证环境(QAS)成功验证后，再从开发环境(DEV)转移到生产环境(PRD)。

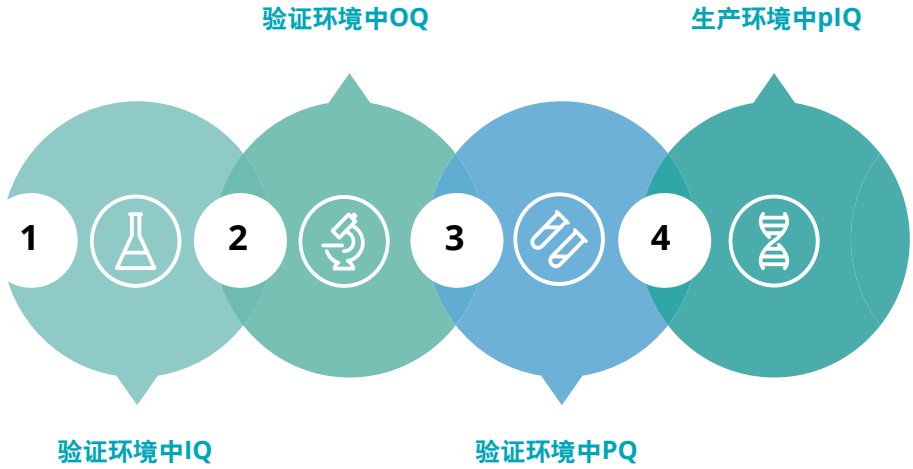
验证将使用V字模型。该模型是使系统在整个生命周期实现合规与符合预定用途的通用方法。该模型的验证过程包括用户需求规范、功能需求规范、设计规范、设计确认、安装确认、运行确认和性能确认。测试阶段的验证活动用来确认规范阶段的需求得到满足。验证工作基于GAMP5，确认工作基于GAMP GPG进行了规划，验证方法如下图所示：

**图3: 使用V字模型的验证方法**



在SAP的验证过程中，首先通过对业务流程进行全面的分析，得到用户需求说明(URS)并映射到功能说明(FS)。配置说明(CS)和设计说明(DS)作为技术的说明文件，阐述了系统实施的技术细节。在每个阶段，FS，CS、DS 和AO将只覆盖该阶段的实施开发范围。设计确认报告(DQ Report)是一个关键节点，标志设计阶段的完成。对于开发的代码中较高风险的，代码审查必须文档化，以确保其符合行业内标准。SAP的定制化和编码过程依据GAMP5中的相关指导。

需要进行所有关于业务流程的系统配置(定制化、开发、权限设置和配置)的确认工作。确认将遵循以下顺序：




确认的执行会按照具体的确认方案进行确认，验收标准等具体信息将会在相关的确认方案中描述。

在亚马逊云上基础架构上搭建新的SAP系统，首先保证云上基础架构为确认合格的状态，然后进行SAP系统的实施和验证。

### 迁移已有SAP系统到亚马逊云上基础架构

将现有SAP系统从传统IT基础架构迁移到亚马逊云端，如何保证数据迁移的合规性？除对云上基础架构进行确认和对SAP系统进行配置、关键功能、业务流程的验证外。验证时还要考虑系统迁移带来的数据迁移的风险的评估。应根据风险评估结论，对数据迁移进行验证，以保证法律法规对数据完整性的要求。

### 功能保持不变，只迁移数据

数据可以通过LSMW,定制的事务代码或者人工方式录入系统。LSMW 是SAP标准功能，使用 Excel/txt 文件来映射和导入验证环境和生产环境的主数据。LSMW 可以组织数据迁移项目，利用其清晰的步骤顺序引导用户完成数据迁移。该工具是SAP标准安装的一部分，它不会被显式验证，但是会对数据迁移进行验证以确保数据被正确的导入。如果定制化的事务代码被用于将主数据迁移到验证环境和生产环境，并在业务实践过程中持续使用，该事务代码将需要进行验证。人工方式为工作人员参照操作流程进行主数据手工录入，需要在PQ过程中验证该流程的可用性。

### 功能保持不变，只升级软件版本

将执行回归测试以确认软件版本的升级未对现有软件功能产生负面影响。

### 功能保持不变，底层基础架构（技术层面）发生改变

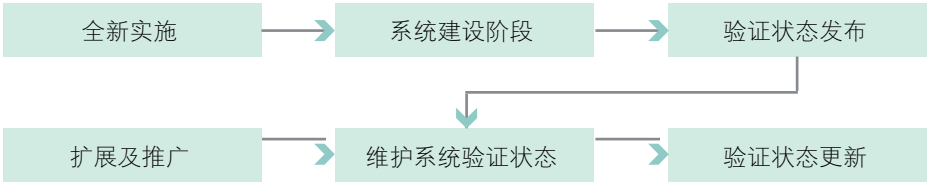
将评估上层功能是否经过验证，如果没有则参考下文中“计算机化系统验证流程及原则”，如果已经经过验证，那将只验证有更改的部分。

## SAP系统计算机化系统验证的最佳实践案例分享

本节将通过展示云上部署应用的计算机化系统验证验证实践案例，来具体说明德勤计算机化系统验证的框架及方法论。

### 计算机化系统验证流程及原则

在SAP系统计算机化系统验证的实施过程中，德勤会根据不同项目CSV验证的范围和策略将其按照全新实施或扩展推广进行划分。




针对全新实施的项目，系统建设阶段中首先会对系统进行GxP相关性评估及风险评估，再根据制药行业相关政策、标准与既定程序制定验证策略。验证策略拟定后，将制定详细的验证计划并确定相关文档模板。所有验证活动的参与者都需要经过系统化培训，培训的全流程将被记录。德勤团队通过详细的基础设施确认方案和用户需求文档，大幅提高了扩展及推广阶段的回归测试速度。此外，团队还通过审查数据迁移与验证方案，并完成可追溯矩阵等记录文件来保证计算机化系统验证的顺利进行。

在与某国际化生物技术公司的合作项目中，实施团队采用了高效、严谨、灵活的德勤CSV方法论以确保计算机化系统合规，根据客户质量管理要求灵活调整细节方法，将风险评估贯穿整个项目的始终。基于Hybrid Agile的方法论，实施团队灵活应对用户需求，以高透明度的交付体系来保证用户的参与度。例如团队把实现阶段分为2次迭代，第一次迭代是基于DLIFE行业蓝图确认的基础功能和流程，这部分特点是：标准为主，差异少或影响小可快速确认，必要的少量开发可以直接使用DLIFE资产或快速完成开发。因此这部分迭代功能可以快速完成第一轮DQ；第二次迭代是在第一次迭代基础上，需要专门定制设计开发的，且周期较长的功能和流程，这部分可以集中在一起作为第二次迭代完成DQ。通过这种方式，一定程度上提升了项目交付效率，在DQ之前充分考虑到了交付的敏捷性，也兼顾保障了CSV合规的要求。

针对扩展或推广项目，德勤团队将通过回顾验证记录，评估IT管理相关SOP和现有验证状态后，为不同的用户需求提供定制化的验证解决方案，包括但不限于：发起变更申请，针对变更进行风险评估/GxP相关性评估，进行差距评估，根据政策、行业标准与既定程序制定验证策略，维护系统已有的验证状态，对变更涉及到的已有功能进行回归测试，完善追溯矩阵等。

在维护系统验证期间的文件的变更、偏差、培训需要遵照严格的流程：

- 验证期间出现的偏差需要调查并配对CAPA，某一阶段的测试偏差关闭后才能进入到下一个测试阶段。例如OQ阶段的偏差完全关闭后，才能进行OQ报告的签署，仅当OQ报告签署完成后，才可进入PQ阶段；
- 文件的变更需要遵循严格的变更流程，提出变更申请后，德勤团队将通过补充测试、培训、文件升级等来保障变更的顺利进行；

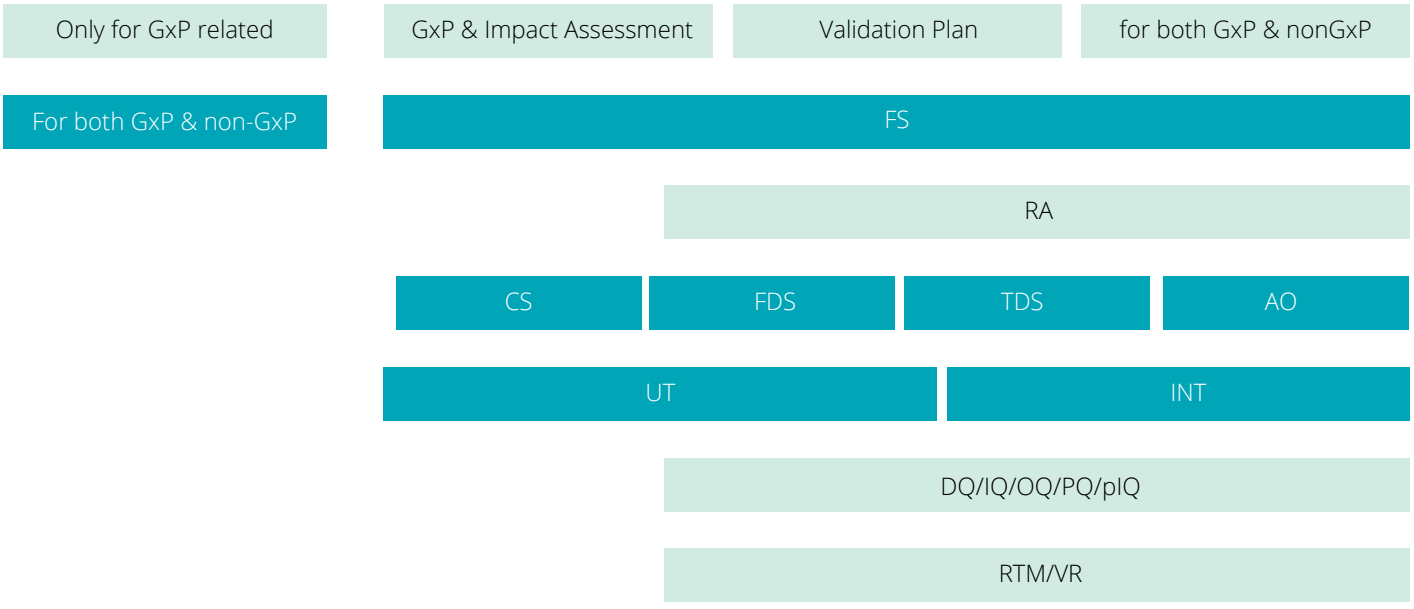
## 计算机化系统验证的交付物

- 概念阶段
  - 验证计划：定义项目中计算机化系统验证的范围、策略以及方法论、交付物、角色职责、签批矩阵、以及可接受标准；
  - URS：从用户的角度来描述验证范围内的业务流程，URS的起草要求客观性、一致性、可测试性、以及唯一性。
- 设计阶段
  - 功能规范文档：功能规范分为配置功能、标准功能、开发功能；功能规范将对应URS，描述该功能是通过何种方式实现的。
  - 风险评估报告
  - ER/ES评估报告
  - 配置规范
  - 功能设计规范：描述开发功能所需的界面和逻辑。
  - 功能技术规范：描述通过何种方式来实现设计规范的界面和逻辑。
  - 设计确认报告：通过对于URS、功能规范、配置规范、设计规范的追溯来在纸面上确保，用户需求通过功能、配置、二次开发来逐一实现。
  - 权限设计
- 测试阶段
  - 源代码审核报告
  - 单元测试/集成测试报告
  - 传输清单
  - 安装确认方案/脚本/报告
  - 运行确认方案/脚本/报告
  - 性能确认方案/脚本/报告
  - 生产环境的安装确认方案/脚本/报告
- 部署阶段
  - 数据迁移计划/报告
  - 需求追溯矩阵
  - 验证报告

## 计算机化系统验证的实践经验总结

- 明确验证活动的范围
  在验证执行前需要对项目进行GxP相关性评估，以确定验证范围。针对业务模块的验证范围，一般情况如下：
  - FI，CO一般不属于验证范围；
  - QM，PP一般属于验证范围；
  - SD，MM需要根据实际情况分析

  针对通用性功能，例如密码策略、用户管理、备份还原、审计追踪、接口配置等功能属于验证范围内，并且有可能穿梭在各模块的测试中，例如审计追踪、接口等。
- 明确项目文件和验证文件的区别
  - 单元测试、集成测试是在开发环境中，属于项目测试，但不属于验证范围，无需遵从计算机化系统验证的培训、偏差、变更管理；
  - 验证环境下的3Q以及生产环境的IQ，属于验证中的测试活动；
  - URS、FS、CS、DS这些文件是即用于项目，又用于验证的，我们需要对其进行合理的区分。对于GxP模块的文件，我们需要按照验证的标准来起草和签批，使其既满足验证要求，也能用做项目文件。而对于非GxP的模块，我们只需要按照项目的要求起草和签批这些文件即可，从而科学有效地减少文件起草数量；



- 正确定义相关方的识别、验证角色及职责
  正确的识别相关方并且定义职责是项目成功的基石。在项目开启时会识别相关方，同时在验证计划中我们也会定义角色和职责。这里的角色和职责在验证活动中最直观的体现，就是对于文件的起草、审核、签批，测试的执行、复核分别由谁来执行。既不能遗漏相关方造成职责的缺失，也不能引入过多的相关方造成项目推进的延迟。
- 正确识别GxP相关的ER/ES
  需要针对识别的ER／ES进行审计追踪的开启，并进行正确的权限分配 (创建、修改、查询、废除) , GxP相关的ER／ES包括配方、供应商执照、客户执照、请验单、质量检验报告书及批生产记录等。
- 全流程的风险管理
  - 初始风险分析：即在项目的概念阶段就需要判定哪些模块是GxP相关，以确定我们的项目范围；
  - 功能风险分析：根据国际通用的一款风险分析工具FMEA，从风险的可能性、严重性、可发现性去确定每一项需求的风险优先级。并根据风险优先级来确定风险减缓措施，其中包括验证活动。
  - 影响评估：影响评估大部分情况下会和功能风险分析合并，二者的区别在于功能风险分析的目的是确定测试的方法，而影响评估多是针对在二期项目以后的项目。需要评估增加的模块或者需求对已有的流程、功能、数据的影响，以确定回归测试的方法和内容。
  - 数据迁移的风险评估：因为迁移的数据的重要性不同会导致数据比对抽样方式的不同，所以数据迁移的风险评估不一定是一个独立的文件，可能是包含在迁移方案中的。需要明确的是这里对于数据的重要性评估不是基于GxP，而是基于业务流程。例如一些财务数据，属于非GxP数据，但是对于业务流程来说非常关键的数据，我们会提高数据比对的抽样比例，例如生产主数据的关键性是非常高的，因此我们需要对其中所有的数据进行比对。反之，针对非关键性的数据，我们会降低数据比对的抽取比例。

德勤团队通过与国内外众多制药行业客户的合作，积累了丰富的行业经验，并完善了德勤计算机化系统验证的框架，为制药行业客户提供了一个预先构建的资产库，在减少SAP项目实施阶段工作量的同时，降低了项目交付风险。


MEDICAL
Health Care
Doctor
Hospital
Pharmacist
Nurse
Dentist
First Aid
Surgeon

# 4. 结论

为应对云计算带来的合规性挑战，使用云平台部署应用的医药企业，不仅应对云上基础架构和云上应用根据法律法规要求进行充分的确认和验证，还应该针对云上基础架构的搭建、验证和确认、运行和维护建立相应的质量管理体系，或者将其纳入到自身已有的计算机化系统质量管理体系中。确保云上基础架构、云上服务、业务应用的合理管控，以应对法律法规对云上计算机化系统合规性、数据完整性的要求。

# 5. 参考


- ISPE, GAMP Good PracticeGuide: IT Infrastructure Control and Compliance
- ISPE, GAMP5 A Risk-Based Approach to Compliant GxP Computerized Systems
- NMPA, 《药品生产质量管理规范 (2010年修订) 》附录《计算机化系统》和《确认与验证》

# 6. 公司简介

## 亚马逊云科技简介

自2006年以来，亚马逊云科技一直是世界上服务丰富、应用广泛的云服务平台。亚马逊云科技提供超过200项全功能的服务，涵盖计算、存储、数据库、联网、分析、机器人、机器学习与人工智能、物联网、移动、安全、混合云、虚拟现实与增强现实、媒体，以及应用开发、部署与管理等各个方面，遍及25个地理区域的80个可用区 (AZ) 。全球数百万客户，包括发展迅速的初创公司、大型企业和领先的政府机构都信赖亚马逊云科技，通过亚马逊云科技的服务强化其基础设施，提高敏捷性，降低成本。

亚马逊云科技在中国有北京和宁夏两个区域。为保证更好的用户体验并遵守中国的法律法规,亚马逊在中国与持有相关电信牌照的本地合作伙伴开展技术合作，由本地合作伙伴向客户提供云服务。北京光环新网科技股份有限公司是亚马逊云北京区域云的服务运营方和提供方，宁夏西云数据科技有限公司是亚马逊云宁夏区域云的服务运营方和提供方。亚马逊云科技、光环新网和西云数据致力于为中国的软件开发人员和企业提供安全、灵活、可靠且低成本的IT基础设施资源，帮助他们实现创新和快速扩大企业规模。亚马逊云科技在中国已发布了大数据、人工智能、物联网等领域涵盖计算、存储、数据库、网络以及安全管理的100多种云服务，并且还在持续扩展中。

## 亚马逊云科技中国的合规遵从

目前北京区域和宁夏区域满足如下的合规资质，并在持续不断增加：

**表4：亚马逊云在中国的合规遵从**

| 北京区域 | 宁夏区域 |
| --- | --- |
| • 等级保护三级<br>• ISO/IEC27001<br>• 可信云服务认证<br>• ISO9001<br>• ISO22301<br>• ISO20000<br>• ISO27018<br>• SOC<br>• PCI-DSS | • 等级保护三级<br>• ISO/IEC27001<br>• 可信云服务认证<br>• ISO9001<br>• ISO22301<br>• ISO27018<br>• SOC<br>• PCI-DSS |

17 访问 https://aws.amazon.com/cn/about-aws/global-infrastructure/以获得关于亚马逊云科技基础设施的准确的最新信息。

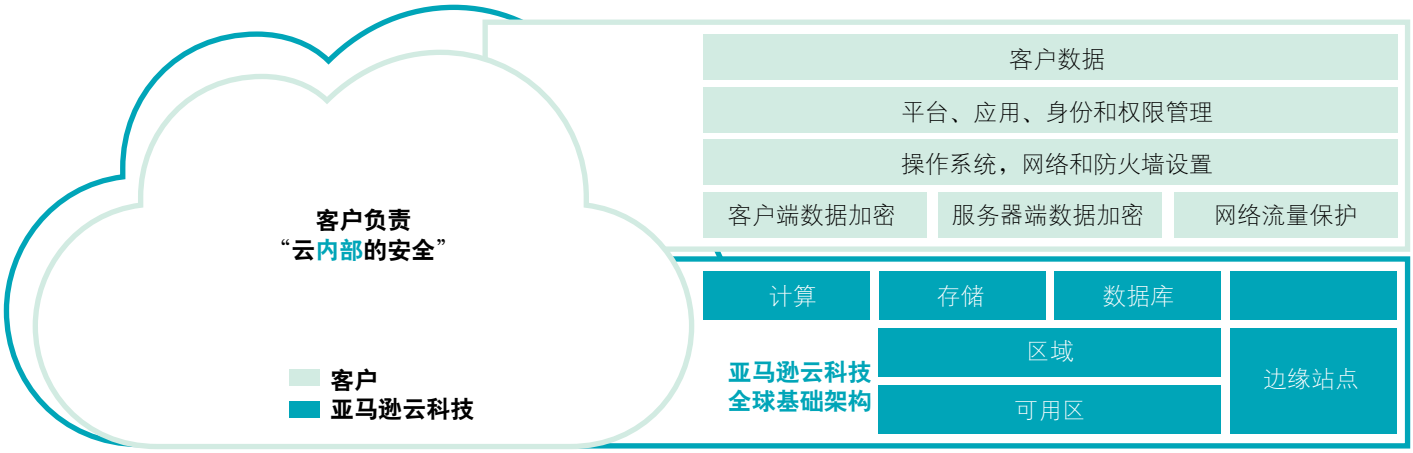
越来越多的制药企业为了降低IT基础设施的拥有和运行成本，在扩展新业务时，将系统部署到亚马逊云科技云上的基础架构。或者当自身拥有和维护的传统IT基础设施不再能够满足业务发展需求时，将已有的业务系统从传统IT基础设施迁移到亚马逊云上。

根据我国2015年颁布的《药品生产质量管理规范（2010年修订）》附录《计算机化系统》第六条，“计算机化系统验证包括应用程序的验证和基础架构的确认”，在亚马逊云上构建制药行业应用，是将亚马逊云上基础架构作为应用运行的基础。为保障上层应用的可用性、安全和性能，对云上基础架构进行验证和确认，以及维持控制和确认的状态至关重要。同样，使用云上基础架构作为上层GxP应用的环境，云上基础架构的确认和维持确认的状态是在云端部署业务系统的先决条件。

### 安全责任共担模型

使用亚马逊部署工作负载，需要首先明确安全合规的责任边界划分。下图显示了亚马逊的安全责任共担模型。

**图4：亚马逊云科技和客户的责任共担模型**




安全性和合规性是亚马逊云科技和客户的共同责任。这种共担模式可以减轻客户的运营负担，因为亚马逊云科技负责运行、管理和控制从主机操作系统和虚拟层到服务运营所在设施的物理安全性的组件。客户负责管理来宾操作系统（包括更新和安全补丁）、其他相关应用程序软件以及亚马逊云科技提供的安全组防火墙的配置。客户应该仔细考虑自己选择的服务，因为他们的责任取决于所使用的服务以及这些服务与其 IT 环境的集成以及适用的法律法规。责任共担还为客户提供了部署所需要的灵活性和控制力。如下图所示，这种责任区分通常涉及云“本身”的安全和云“内部”的安全。

- 亚马逊云科技负责“云本身的安全”—— 亚马逊云科技负责保护运行所有亚马逊云科技云服务的基础设施。该基础实施由运行亚马逊云服务的硬件、软件、网络和设备组成。
- 客户负责“云内部的安全”—— 客户责任由客户所选的亚马逊云服务确定。这决定了客户在履行安全责任时必须完成的配置工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 等服务被归类为基础设施即服务 (IaaS)，因此要求客户执行所有必要的安全配置和管理任务。部署 Amazon EC2 实例的客户需要负责来宾操作系统（包括更新和安全补丁）的管理、客户在实例上安装的任何应用程序软件或实用工具，以及每个实例上 亚马逊云科技提供的防火墙（称为安全组）的配置。对于抽象化服务，例如 Amazon S3 和 Amazon DynamoDB，亚马逊云科技运营基础设施层、操作系统和平台，而客户通过访问终端节点存储和检索数据。客户负责管理其数据（包括加密选项），对其资产进行分类，以及使用 IAM 工具分配适当的权限。

## 德勤简介

成立于1833年的德勤是全球最大的专业服务机构，超过30万名全球员工资源可以全球项目共享，德勤(Deloitte)是在企业管理咨询、财务/税务咨询、审计方面全球最大的专业型服务公司，提供世界顶尖水准的审计、企业管理与业务流程优化咨询、财务和税务咨询服务；客户包括大型跨国企业、大型国有企业，同时还有众多的公共机构，以及更多快速成长的中小型企业。德勤所具有的跨国业务经验可以支持无论客户在哪里运作，德勤都可以为客户提供高水平的专业服务。

德勤中国的事务所网络,在德勤全球网络的支持下,为中国的本地、跨国及高增长企业客户提供全面的审计、税务、企业管理咨询及财务咨询服务。德勤中国生命科学与医疗行业拥有一支由专业人士组成的精英团队。不同的文化背景、精湛的专业技能以及对中国行业挑战的认识让这支队伍能够更有效的与客户进行沟通、更准确的掌握客户的需求，更全面的为客户提供各种解决方案。

德勤在中国主要提供企业管理咨询、税务、审计、财务咨询、企业风险管理服务。德勤咨询是SAP铂金级优秀合作伙伴，德勤咨询在所有主要行业和关键产品上与SAP建立了紧密的战略协同，以充分利用专业咨询服务的行业经验和客户影响力，大力在客户端推进SAP关键技术，以支持客户进行数字化转型，云转型和数字创新。德勤咨询在协助客户业务转型方面的杰出能力和领先地位，具体表现在以下各个方面：

- 在数字化转型领域保持ERP实施项目数量领先，并积极配合SAP开展各领域合作；
- 大量大型ERP实施项目成功实施上线经验；
- 在云转型领域，德勤咨询合作实施多个S/4 HANA项目，助力数字化转型。

在计算机化系统验证方面，德勤通过多年的海内外制药行业计算机化系统验证项目经验的积累和沉淀，形成了一套切实可行、适合当地行业特点的计算机化系统验证验证方法论。德勤的计算机化系统验证验证方法论与德勤SAP实施方法论无缝整合，从效率、成本、质量三方面保障系统的合规与项目的成功。德勤是在SAP系统实施领域和计算机化系统验证验证领域都拥有成熟团队的咨询公司。德勤验证团队具有大型国际制药企业SAP实施和验证经验。

# 7. 缩写

| 定义/缩写 | 描述 |
| --- | --- |
| **APP** | Application on Mobile<br>移动设备上的应用 |
| **AO** | Authorization<br>权限设计 |
| **CS** | Configuration Specification<br>配置说明书/标准 |
| **CAPA** | Corrective Action and Preventive Action<br>纠正措施和预防措施 |
| **DQ** | Design Qualification<br>设计确认 |
| **ERP** | Enterprise Resource Planning<br>企业资源计划系统 |
| **FDA** | Food and Drug Administration<br>美国食品药物管理局 |
| **FS** | Functional Specification<br>功能说明书 |
| **FDS** | Functional Design Specification<br>功能设计规范 |
| **GMP** | Good Manufacturing Practice<br>良好生产规范 |
| **GAMP** | Good Automated Manufacturing Practices<br>良好的自动化生产实践 |
| **GxP** | Good x (Manufacturing, Clinical, Laboratory…) Practice<br>(制造，临床，实验室)的良好实践 |
| **INT** | Integration Test<br>集成测试 |
| **IQ** | Installation Qualification<br>安装确认 |
| **IT** | Information Technology<br>信息技术 |
| **LSMW** | Legacy System Migration Workbench<br>遗留系统移植平台 |
| **OQ** | Operational Qualification<br>运行确认 |

| 定义/缩写 | 描述 |
| --- | --- |
| **pIQ** | Production Environment Installation Qualification<br>生产环境安装确认 |
| **PQ** | Performance Qualification<br>性能确认 |
| **SAP** | Systems, Applications Products<br>SAP公司的产品——企业管理解决方案的软件名称 |
| **SAP S/4HANA** | SAP S/4HANA is a set of SAP business suit 4<br>系统应用产品，S/4HANA 为SAP系统的套装组件4 |
| **SOP** | Standard Operation Procedure<br>标准操作程序 |
| **TDS** | Technical Design Specification<br>技术设计规范 |
| **RTM** | Traceability Matrix<br>追溯矩阵 |
| **UT** | Unit Test<br>单元测试 |
| **URS** | User Requirement Specification<br>用户需求说明书 |
| **VR** | Validation Report<br>验证报告 |
| **VPL** | Validation Plan<br>验证计划 |
| **亚马逊云科技** | Amazon Web Service<br>亚马逊云计算服务平台 |
| **计算机化系统验证** | Computerized System Validation<br>计算机化系统验证 |

# 8. 致谢


## 指导及主编人员

**德勤：**

周令坤、黎涛、朱昊、曹营杰、张婧娱

**亚马逊云科技：**

韩旭明、黄庆春、周德标、包光磊、张亮

Designed by CoRe Creative Services. RITM0816705